Effective Siegel's Theorem for Modular Curves

Yuri Bilu*, Marco Illengo*

February 25, 2010

Abstract

We prove that integral points can be effectively determined on all but finitely many modular curves, and on all but one modular curve of prime power level.

Contents

1 Introduction

Let X be a curve defined over a number field K and $j \in K(X)$ a K-rational function on X. Let also R be a subring of K. We define the set $X(R, j)$ of R-integral points on X with respect to j by

$$X(R, j) = \{P \in X(K) : j(P) \in R\}.$$

The following fundamental theorem was proved by Siegel in 1929.

Theorem 1.1 (Siegel [15]) *Assume that either* $\mathbf{g}(X) \geqslant 1$ *or* j *has at least* 3 *distinct poles. Then for any finitely generated subring* R *of* K *the set* $X(R, j)$ *is finite.*

Siegel himself considered only the case $R = \mathcal{O}_K$, but the extension to general R is relatively straightforward (see [12, 14]). Recently Corvaja and Zannier [6] gave a new beautiful proof of Siegel's theorem, which extends to higher dimensions.

Theorem 1.1 admits the following converse: if $\mathbf{g}(X) = 0$ and j has at most 2 distinct poles, then, for some finite extension K' of K, and some finitely generated subring R' of K', the set $X(R', j)$ is infinite. See [1] for a more precise statement.

For curves of genus at least 2, Faltings [8] improved on the Theorem of Siegel by showing that $X(K)$ is finite if $\mathbf{g}(X) \geqslant 2$.

Both the results of Siegel and Faltings are *non-effective*, that is, neither of them provides any bound for the size of the points in $X(R, j)$ computable in terms of X, j, K and R.

Let X be a curve defined over $\bar{\mathbb{Q}}$ and $j \in \bar{\mathbb{Q}}(X)$ a non-constant rational function on X. We call the couple (X, j) *Siegelian* if one of the conditions of Siegel's Theorem is satisfied, that is: either $\mathbf{g}(X) \geqslant 1$ *or* j has at least 3 distinct poles. Thus, the couple is non-Siegelian if X is of genus 0 *and* j has at most two poles. We say that *Siegel's theorem is effective* for a Siegelian couple (X, j) if for any number field K such that the couple (X, j) is defined over K, and for any finitely generated subring R of K, the set $X(R, j)$ (which is finite by the Theorem of Siegel) can be effectively determined in terms of X, j, K and R.

Starting from pioneering work of A. Baker, there have been obtained effective versions for some cases of this theorem; see [4, 5] for the history of the subject and further references. For instance, the following is known.

*Université Bordeaux 1

Theorem 1.2 *Siegel's theorem is effective for (X, j) if*

1. (folklore) $\mathbf{g}(X) = 0$ *and j has at least 3 poles, or*
2. (Baker and Coates [2]) $\mathbf{g}(X) = 1$, *or*
3. (Bilu [3], Dvornicich and Zannier [7]) $\mathbf{g}(X) \geqslant 1$ *and $\bar{K}(X)/\bar{K}(j)$ is a Galois extension.*

Starting from [4], Baker's method is applied to obtain effective Siegel's theorem for various classes of modular curves. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and X_Γ the corresponding modular curve. (See Subsection 1.1 for the definitions.) As usual, we denote j the modular invariant function. The couple (X_Γ, j) is defined over $\bar{\mathbb{Q}}$, and one can study the Diophantine properties of this couple. In particular, on can ask the following question:

assuming the couple (X_Γ, j) Siegelian, is Siegel's theorem effective for this couple?

In the sequel, we call a modular curve X_Γ (non-)Siegelian if the couple (X_Γ, j) is (non-)Siegelian, where j is the modular invariant. We shall say that *Siegel's theorem is effective* for a Siegelian X_Γ if it is effective for the couple (X_Γ, j).

In [4, 5] Siegel's theorem was shown to be effective for several classes of modular curves, like the curves $X(n)$, $X_1(n)$ and $X_0(n)$ (provided they are Siegelian). For $X(n)$ effective Siegel's theorem was already established by Kubert and Lang [9, Section 8.1] (they do not make any mention of effectiveness, but it is implicit in their work). The results of [4, 5] are based on the "three cusps criterion", see Section 2.

In the present article we show that Siegel's theorem is effective for all but finitely many X_Γ, and for all but one X_Γ of prime power level. Our principal results are the following two theorems.

Theorem 1.3 *Let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of prime power level, distinct from 25. Then either X_Γ is non-Siegelian, or Siegel's theorem is effective for X_Γ.*

At level 25 there is a subgroup Γ, defined in Proposition 4.18, for which the curve X_Γ is of genus 2 and for which our argument does not work.

Theorem 1.4 *Let Γ be a subgroup of level not dividing the number $2^{20}\cdot 3^7\cdot 5^3\cdot 7^2\cdot 11\cdot 13$. Then Siegel's theorem is effective for X_Γ.*

The assumption on the level in Theorem 1.4 can certainly be relaxed, but at the moment, the methods of the present article do not allow treatment of certain Siegelian modular curves of small mixed level. Consider, for instance, two congruence subgroups Γ_5 and Γ_7 of levels 5 and 7, whose projections to $\mathrm{PSL}_2(\mathbb{F}_5)$ and $\mathrm{PSL}_2(\mathbb{F}_7)$ (see Table 1(a)) are isomorphic to the fourth alternating group $\mathcal{A}_4$ and to the fourth symmetric group $\mathcal{S}_4$, respectively; their intersection $\Gamma_5 \cap \Gamma_7$ is a congruence subgroup Γ of the level 35 such that X_Γ has genus 2. This X_Γ is non-Siegelian, but eludes our methods.

1.1 Notation and Conventions

We denote by $\mathcal{C}_n$ the n-th cyclic group, and by $\mathcal{D}_n$ the n-th dihedral group (so that $\mathcal{C}_n$ is the index 2 subgroup of $\mathcal{D}_n$). Further, we denote by $\mathcal{S}_n$ and $\mathcal{A}_n$ the n-th symmetric and alternating groups, respectively.

The letter Γ is reserved to congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, that is, subgroups containing $\Gamma(n)$ for some n. We shall say in this case that Γ is of *level dividing* n. The smallest n with this property will be called the *exact level* of Γ.

Fix a positive integer n. Then to any congruence subgroup Γ of level dividing n we associate a subgroup G of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ and a subgroup $\bar{G}$ of $\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z})$, as the images of Γ under the natural maps $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z})$. Conversely, Γ is uniquely determined by G (and n). When n is 2, 4 or p^k with an odd prime p, then Γ is uniquely determined by $\bar{G}$, under the additional assumption that $\Gamma \ni -I$. In the sequel, when n is fixed, we shall freely interchange between Γ and G, when it causes no confusion. Also, when the additional assumptions indicated above are satisfied, we shall interchange between Γ, G and $\bar{G}$.

We use the common notation $\nu_2(\Gamma)$, $\nu_3(\Gamma)$, $\nu_\infty(\Gamma)$ and $\mu(\Gamma)$ for, respectively, the number of the 2-elliptic points of Γ, the number of its 3-elliptic points, the number of its cusps, and the index $[\mathrm{PSL}_2(\mathbb{Z}) : \bar{\Gamma}]$, where $\bar{\Gamma}$ is the image of Γ in $\mathrm{PSL}_2(\mathbb{Z})$.

The modular curve X_Γ is, by definition, the quotient $\Gamma\backslash\bar{\mathcal{H}}$ (where $\bar{\mathcal{H}}$ is the extended Poincaré upper half-plane), with properly defined topology and analytic structure. The modular invariant j defined a non-constant rational function on X_Γ, whose poles are exactly the cusps. While defined analytically, the curve X_Γ, or, more precisely, the couple (X_Γ, j) has a model over $\bar{\mathbb{Q}}$ (even over $\mathbb{Q}(\zeta_n)$, where n is the level of Γ). See any standard reference like [11, 16] for all the missing details.

1.2 Plan of the Article

In Section 2 we state our main tool, the "three cusps criterion", and obtain some auxiliary results on the cusps to be used throughout the article. In Section 3 we study curves of the prime level, and show that for them Siegel's theorem is effective whenever they are Siegelian; we also classify the non-Siegelian curves of prime level. In Section 4 we do the same for the curves of prime power level (with the aforementioned exception at level 25). In Section 5 we consider mixed levels.

Acknowledgments We thank Roberto Maria Avanzi and Michael Stoll for useful discussions, and for performing, at our request, electronic calculations that helped our intuition. We also thank Pierre Parent for useful discussions.

2 The "Three Cusps Criterion"

The following theorem (see [4]) plays a capital role in the present article.

Theorem 2.1 *Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Then Siegel's theorem is effective for X_Γ if the group Γ has at least 3 cusps.*

We shall also use the following refinement of Theorem 2.1, see [5, Proposition 12].

Theorem 2.2 *Let Γ have a congruence subgroup Γ', which contains all elliptic elements of Γ and has at least 3 cusps. Then Siegel's theorem is effective for X_Γ.*

Applying Theorems 2.1 and 2.2 requires computing (or estimating) the number of cusps $\nu_\infty(\Gamma)$ of a congruence subgroup Γ. For this purpose we shall use the following simple lemma. It is certainly known, but we could not find a proof in the literature.

For any natural n we denote by $\mathcal{M}_n$ the set of elements of exact order n in $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Obviously,

$$|\mathcal{M}_n| = n^2 \prod_{p|n} \left(1 - p^{-2}\right), \tag{1}$$

the product being taken over all primes p dividing n.

Lemma 2.3 *Let Γ be a congruence subgroup of level dividing n and containing $-I$, and let G be the projection of Γ modulo n. Then the number $\nu_\infty(\Gamma)$ is equal to the number of the orbits of the natural (left) G-action on $\mathcal{M}_n$. In symbols, we have $\nu_\infty(\Gamma) = |G\backslash\mathcal{M}_n|$.*

Proof – The number $\nu_\infty(\Gamma)$ equals the number of Γ-orbits of $\mathbb{P}_1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ and, since Γ contains $-I$, is also the number of Γ-orbits in the set $\mathcal{M}$ of coprime couples $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. It will suffice to prove that $\mathcal{M}_n$ corresponds to the set of $\Gamma(n)$-orbits of $\mathcal{M}$, where $\Gamma(n)$ is the principal congruence subgroup of level n, i.e. the kernel of the reduction map $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

First, let $\binom{a}{b} \in \mathcal{M}$ be any representative of $\binom{1}{0} \in \mathcal{M}_n$, that is, let a and b be any two coprime integers with $a \equiv 1 \pmod{n}$ and $b \equiv 0 \pmod{n}$. As a and b are coprime, there exist integers x and y such that $ax + by = 1$. Note that $x \equiv 1 \pmod{n}$. Then the matrix $M = \left(\begin{smallmatrix} x+by & y-ay \\ -b & a \end{smallmatrix}\right)$ lies in $\Gamma(n)$ and maps $\binom{a}{b}$ to $\binom{1}{0}$. This shows that the $\Gamma(n)$-orbit of $\binom{1}{0}$ is the class of all representative of $\binom{1}{0} \in \mathcal{M}_n$. We conclude by the transitivity of $\mathrm{SL}_2(\mathbb{Z})$ over $\mathcal{M}$ and by the normality of $\Gamma(n)$ in $\mathrm{SL}_2(\mathbb{Z})$. □

Corollary 2.4 *Let Γ and G be as in the proposition. Assume that Γ has at most 2 cusps. Then $|G| \geqslant |\mathcal{M}_n|/2$.* □

3 The Prime Levels

In this section we classify the non-Siegelian modular curves of prime level, and prove effective Siegel's theorem for Siegelian curves of prime level.

Theorem 3.1 *1. All the Γ (up to conjugacy) of exact prime level, for which X_Γ is non-Siegelian, are listed in Tables 1(a) and 1(b) on page 5.*

2. Let Γ be a congruence subgroup of prime level such that X_Γ is Siegelian. Then Siegel's theorem is effective for X_Γ.

3.1 Lemmas

Here we collect basic properties of the special linear group $\mathrm{SL}_2(\mathbb{F}_p)$. The following property is well-known but we sketch a proof for the sake of completeness.

Proposition 3.2 *The order of an element of $\mathrm{SL}_2(\mathbb{F}_p)$ is either $2p$ or at most $p+1$. When $p \neq 2$, the order of an element of $\mathrm{PSL}_2(\mathbb{F}_p)$ is either p or at most $(p+1)/2$.*

Proof – A matrix from $\mathrm{SL}_2(\mathbb{F}_p)$ is either similar over $\mathbb{F}_p$ to $\left(\begin{smallmatrix}\lambda & 1\\ 0 & \lambda\end{smallmatrix}\right)$ with $\lambda = \pm 1$ or similar over $\mathbb{F}_{p^2}$ to $\left(\begin{smallmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{smallmatrix}\right)$ with $\alpha \in \mathbb{F}_{p^2}$. In the first case the order divides $2p$. In the second case either $\alpha \in \mathbb{F}_p$, in which case the order divides $p-1$, or α is in the kernel of the norm map $\mathbb{F}_{p^2} \to \mathbb{F}_p$, in which case the order divides $p+1$. □

We shall systematically use the classification of semi-simple subgroups of $\mathrm{PSL}_2(\mathbb{F}_p)$. Actually, a classification for $\mathrm{PGL}_2(\mathbb{F}_p)$ is available, see [13, Proposition 16].

Proposition 3.3 *Let $\bar{G}$ be a proper subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$ of order not divisible by p. Then $\bar{G}$ is isomorphic to one of the following groups:*

- *$\mathcal{C}_n$, the n-th cyclic group;*
- *$\mathcal{D}_n$, the n-th dihedral group;*
- *$\mathcal{A}_4$, the fourth alternating group;*
- *$\mathcal{S}_4$, the fourth symmetric group;*
- *$\mathcal{A}_5$, the fifth alternating group (this only happens when $p \equiv \pm 1 \pmod 5$).*

In the unipotent case, one has the following, see [13, Proposition 15].

Proposition 3.4 *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ of order divisible by p. Then G either contains $\mathrm{SL}_2(\mathbb{F}_p)$ or is contained in a Borel subgroup of $GL_2(\mathbb{F}_p)$.*

(A *Borel subgroup* of $\mathrm{GL}_2(\mathbb{F}_p)$ is a subgroup conjugate to the subgroup $\mathrm{GT}_2(\mathbb{F}_p)$ of the upper-triangular matrices.)

Proposition 3.5 *Let G be a subgroup of the special triangular group $\mathrm{ST}_2(\mathbb{F}_p)$ with $\nu_\infty(G) \leqslant 2$. Then $G = \mathrm{ST}_2(\mathbb{F}_p)$.*

Proof – If G were a proper subgroup of $\mathrm{ST}_2(\mathbb{F}_p)$, then its cardinality would be at most half the cardinality of $\mathrm{ST}_2(\mathbb{F}_p)$, that is, $|G| \leqslant (p^2-p)/2$. On the other hand, $|G| \geqslant (p^2-1)/2$ by Corollary 2.4, a contradiction. □

Theorem 3.6 *Let Γ be a congruence subgroup of exact level p, with at most 2 cusps.*

- *If p does not divide the cardinality of $\bar{G}$ then we are in one of the following eight cases.*

$$\begin{array}{lll} p=2 & \text{and } \bar{G} \cong \mathcal{C}_3; & \\ p=3 & \text{and } \bar{G} \cong \mathcal{C}_2 & \text{or } \mathcal{D}_2; \\ p=5 & \text{and } \bar{G} \cong \mathcal{D}_3 & \text{or } \mathcal{A}_4; \\ p=7 & \text{and } \bar{G} \cong \mathcal{A}_4 & \text{or } \mathcal{S}_4; \\ p=11 & \text{and } \bar{G} \cong \mathcal{A}_5. & \end{array} \tag{2}$$

- *If p divides the cardinality of $\bar{G}$ then G is conjugate to* $\mathrm{ST}_2(\mathbb{F}_p)$ *and* $\nu_\infty(\Gamma) = 2$.

Proof – If $p = 2$ we conclude by inspection. Now assume that $p \geqslant 3$. When $|\bar{G}|$ is not divisible by p, Propositions 3.2 and 3.3 imply the upper bound $|\bar{G}| \leqslant \max\{p+1, 60\}$, and 60 can be replaced by 24 if $p \not\equiv \pm 1 \pmod 5$. On the other hand, Corollary 2.4 implies the lower bound $|\bar{G}| \geqslant (p^2-1)/4$. It follows that $p \leqslant 11$, and we again conclude by inspection. See [10, Theorem 6.1.6] for more details.

When p divides $|\bar{G}|$, Proposition 3.4 implies that either $G = \mathrm{SL}_2(\mathbb{F}_p)$ or G is conjugate to a subgroup of $\mathrm{ST}_2(\mathbb{F}_p)$. In the first case Γ is $\mathrm{SL}_2(\mathbb{Z})$, against our assumption on its level; in the second case we conclude by Proposition 3.5. □

The invariants of the modular curves corresponding to the eight cases (2) are given in Table 1(a). We see that all the corresponding curves are non-Siegelian. We may also remark that in the first five cases (with $p \leqslant 5$) the group $\bar{G}$ is uniquely defined up to conjugacy, and that in each of the last three cases (with $p \geqslant 7$) the group $\bar{G}$ belongs to one of two distinct conjugacy classes, so, up to modular equivalence, Table 1(a) defines 11 modular curves.

Remark that in all the above cases we have $\nu_\infty(G)|G| = |\mathcal{M}_p|$.

When p divides $|G|$ and $\mu_\infty(G) \leqslant 2$, by Theorem 3.6 the either the group G is $\mathrm{SL}_2(\mathbb{F}_p)$, in which case we obtain the non-Siegelian curve $X(1)$, or G is conjugate to $\mathrm{ST}_2(\mathbb{F}_p)$. In this this latter case, up to conjugacy, $\Gamma = \Gamma_0(p)$. The effectivity problem for the modular curves $X_0(n)$ is completely solved in [5, Theorem 10]:

Theorem 3.7 *Given an integer $n > 1$, either Siegel's theorem is effective for $X_0(n)$ or the couple $X_0(n)$ is non-Siegelian, which is the case if and only n is in the set* $\{2, 3, 5, 7, 13\}$. □

The invariants of the corresponding modular curves are given in Table 1(b).

This completes the proof of Theorem 3.1.

Table 1: Non-Siegelian modular curves of exact prime level

(a) The semi-simple case

p	$\bar{G}$	μ	ν_∞	ν_2	ν_3	$\mathbf{g}$	remark
2	$\mathcal{C}_3$	2	1	0	2	0	
3	$\mathcal{C}_2$	6	2	2	0	0	$X_{\text{split}}(3)$
3	$\mathcal{D}_2$	3	1	3	0	0	$X_{\text{nonsplit}}(3)$
5	$\mathcal{D}_3$	10	2	2	1	0	$X_{\text{nonsplit}}(5)$
5	$\mathcal{A}_4$	5	1	1	2	0	
7	$\mathcal{A}_4$	14	2	2	2	0	2 groups
7	$\mathcal{S}_4$	7	1	3	1	0	2 groups
11	$\mathcal{A}_5$	11	1	3	2	0	2 groups

(b) The unipotent case

p	Γ	μ	ν_∞	ν_2	ν_3	$\mathbf{g}$
2	$\Gamma_0(2)$	3	2	1	0	0
3	$\Gamma_0(3)$	4	2	0	1	0
5	$\Gamma_0(5)$	6	2	2	0	0
7	$\Gamma_0(7)$	8	2	0	2	0
13	$\Gamma_0(13)$	14	2	2	2	0

4 The Prime Power Levels

4.1 Introduction

In this section we study groups of prime power level. Our ultimate goal is Theorem 1.3. As in the prime case, our main tool will be "three cusps criterion", in the refined form of Theorem 2.2

We obtain a complete classification, up to conjugacy, of the groups Γ, containing $-I$, that do not satisfy the hypothesis of Theorem 2.2. Notice that the hypothesis of Theorem 2.2 automatically fails for Γ if X_Γ is non-Siegelian. Thus, as a by-product, we classify non-Siegelian modular curves of prime power level. Up to modular equivalence, there are 34 such curves:

- the curve $X(1)$ of level 1;
- 16 curves of prime level, listed in Table 1;
- 17 curves of exact level p^e with $e > 1$, listed in Table 2.

Besides them, there are three more modular curves of prime power level, for which the hypothesis of Theorem 2.2 is not satisfied. Two of them, one of level 27 and the other of level 32, are defined in Propositions 4.13 and 4.21 and have genus 1; for them Siegel's theorem is effective due to Theorem 1.2. The third one, the already mentioned curve of level 25 and genus 2, occurs in Proposition 4.18, and this is the only curve of prime power level for which our argument fails.

4.2 The "Exponential" Map

Let p be a prime number and r, s positive integers. We denote by $\mathrm{M}_2(R)$ the ring of 2×2 matrices over a ring R, and by $\mathrm{sl}_2(R)$ the additive group of traceless 2×2 matrices. We define the "exponential" map

$$\exp = \exp_{r,s} : \mathrm{M}_2(\mathbb{Z}/p^r\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p^{s+r}\mathbb{Z})$$

by $\exp(A) = I + p^s\widetilde{A}$, where $\widetilde{A} \in \mathrm{M}_2(\mathbb{Z}/p^{r+s}\mathbb{Z})$ is a lifting of A; clearly, $\exp(A)$ does not depend on the choice of the lifting. Slightly abusing notation, we shall often write $I + p^sA$ instead of $\exp(A)$.

Proposition 4.1 *Assume that $r \leqslant s$. Then $\exp\bigl(\mathrm{sl}_2(\mathbb{Z}/p^r\mathbb{Z})\bigr) \subset \mathrm{SL}_2(\mathbb{Z}/p^{r+s}\mathbb{Z})$ and we have the short exact sequence*

$$\mathrm{sl}_2(\mathbb{Z}/p^r\mathbb{Z}) \xhookrightarrow{\exp_{r,s}} \mathrm{SL}_2(\mathbb{Z}/p^{s+r}\mathbb{Z}) \xrightarrow{\pi_s} \mathrm{SL}_2(\mathbb{Z}/p^s\mathbb{Z}), \tag{3}$$

where π_s is the reduction modulo p^s.

The proof is immediate because $\det\bigl(I + p^s\widetilde{A}\bigr) = 1 + p^s\mathrm{Tr}\,\widetilde{A} + p^{2s}\det\widetilde{A}$.

4.3 Reductions

Let p be a prime, $q = p^e$ be a power of p, and Γ be a congruence subgroup of exact level q. For a positive integer s we consider the *reduction map* modulo p^s from $\mathrm{SL}_2(\mathbb{Z})$ to $\mathrm{SL}_2(\mathbb{Z}/p^s\mathbb{Z})$; the image of Γ is a subgroup G_s of $\mathrm{SL}_2(\mathbb{Z}/p^s\mathbb{Z})$, whose preimage is a congruence subgroup $\Gamma_s = \Gamma\cdot\Gamma(p^s)$ of level dividing p^s. Then we have a chain of surjective maps

$$\Gamma \twoheadrightarrow \cdots \twoheadrightarrow G_{e+1} \twoheadrightarrow G_e \twoheadrightarrow G_{e-1} \twoheadrightarrow \cdots \twoheadrightarrow G_2 \twoheadrightarrow G_1, \tag{4}$$

and a corresponding nested chain of congruence subgroups

$$\Gamma = \cdots = \Gamma_{e+1} = \Gamma_e \subsetneq \Gamma_{e-1} \subseteq \cdots \subseteq \Gamma_2 \subseteq \Gamma_1.$$

Note that if Γ satisfies the conditions

$$\Gamma \ni -I, \qquad \nu_\infty(\Gamma) \leqslant 2. \tag{5}$$

then so does Γ_s for every s; in particular, the congruence subgroup Γ_1 of level dividing p belongs to the finite set of groups that we have determined in the previous section.

Remark 4.2 One might notice that, while we assume the group $\Gamma = \Gamma_e$ to have the exact level p^e, for the $s \neq e$ the group Γ_s is not obliged to have the exact level p^s (actually, it never does for $s > e$ and sometimes even for $s < e$); *a priori*, we only know that its level divides p^s.

For a positive integer s put $K_{s+1} = \mathrm{Ker}(\pi_s|_{G_{s+1}})$, where the groups G_i are as in (4) and π_s is the reduction modulo p^s. Taking $r = 1$ in (3) we have a short exact sequence

$$\mathrm{sl}_2(\mathbb{F}_p) \xhookrightarrow{\exp_{1,s}} \mathrm{SL}_2(\mathbb{Z}/p^{s+1}\mathbb{Z}) \xrightarrow{\pi_s} \mathrm{SL}_2(\mathbb{Z}/p^s\mathbb{Z}),$$

and by restriction to the subgroup G_{s+1} of $\mathrm{SL}_2(\mathbb{Z}/p^{s+1}\mathbb{Z})$ we obtain a short exact sequence

$$V_s \xhookrightarrow{\exp_{1,s}} G_{s+1} \xrightarrow{\pi_s} G_s, \tag{6}$$

where

$$V_s = \exp_{1,s}^{-1}(K_{s+1})$$

is a subspace of $\mathrm{sl}_2(\mathbb{F}_p)$. Thus, the chain of maps (4) determines a sequence of subspaces $V_1, V_2, \ldots$ of $\mathrm{sl}_2(\mathbb{F}_p)$.

The group $\mathrm{SL}_2(\mathbb{F}_p)$ acts by conjugation on $\mathrm{sl}_2(\mathbb{F}_p)$, which defines a natural action on $\mathrm{sl}_2(\mathbb{F}_p)$ of any subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$, in particular of G_1. The following is immediate.

Proposition 4.3 *The spaces V_s are invariant under the natural action of G_1 on $\mathrm{sl}_2(\mathbb{F}_p)$ defined above.* □

It is crucial that the sequence (V_i) is (non-strictly) increasing, with one little exception.

Proposition 4.4 *If $p^s \neq 2$ then $V_s \subset V_{s+1}$. If $p = 2$ then $V_1 \subset V_2 + \langle I \rangle$.*

Proof – Let M be an element of V_s, so that G_{s+1} contains the element $I + p^s M$. By surjectivity of the projection $\pi_{s+1}\colon G_{s+2} \to G_{s+1}$, there exists a matrix N with entries in $\mathbb{Z}/p^2\mathbb{Z}$ such that $I + p^s N \in G_{s+2}$ projects to $I + p^s M$; obviously, $N \equiv M \pmod p$. In G_{s+2} the p-th power of $I + p^s N$ is

$$(I + p^s N)^p = I + p^{s+1} N + \binom{p}{2} p^{2s} N^2 = I + p^{s+1} \left(N + \binom{p}{2} p^{s-1} N^2 \right),$$

implying that $M + \binom{p}{2} p^{s-1} M^2$ lies in V_{s+1}. If $p \neq 2$ or $s > 1$, then p divides $\binom{p}{2} p^{s-1}$ and therefore $M \in V_{s+1}$. If $p = 2$ and $s = 1$ then $M + M^2$ lies in V_2. Since $\operatorname{Tr} M = 0$ we have $M^2 = -I \det M$, whence $M \in V_2 + \langle I \rangle$. □

Remark 4.5 It is worth mentioning that, when $p = 2$ and $-I \in \Gamma$, we have $I \in V_1$, because $I + 2I = -I$ belongs to G_2.

Corollary 4.6 *Let Γ be a congruence subgroup of the exact level p^e. If $V_s = \mathrm{sl}_2(\mathbb{F}_p)$ for some s, then $e \leqslant s$.*

Proof – For $e > 1$ the hypothesis implies $V_{e-1} \neq \mathrm{sl}_2(\mathbb{F}_p)$. Then it suffices to show that $V_s = \mathrm{sl}_2(\mathbb{F}_p)$ implies $V_{s+1} = \mathrm{sl}_2(\mathbb{F}_p)$. This follows from Proposition 4.4 if $p^s > 2$, and it is verified by inspection for $p^s = 2$. □

Remark 4.7 This corollary implies that the group $\Gamma_s = \Gamma \cdot \Gamma(p^s)$ has the exact level p^s for $1 < s < e$. (See also Remark 4.2.)

Proposition 4.8 *If Γ contains $-I$ and has at most two cusps, then $|G_2| \geqslant (p^4 - p^2)/2$ and $V_1 \neq \langle 0 \rangle$. Under the additional assumption $[\mathrm{SL}_2(\mathbb{F}_p) : G_1] > 2$ we have $\dim(V_1) \geqslant 2$.*

Proof – Let $\mu_1 = \mu(\Gamma_1)$ be the index of G_1 in $\mathrm{SL}_2(\mathbb{F}_p)$. Then $|G_1| = (p^3 - p)/\mu_1$. Since $\nu_\infty(\Gamma) \leqslant 2$, Corollary 2.4 and equation (1) imply $|G_2| \geqslant (p^4 - p^2)/2$. Hence

$$|V_1| = \frac{|G_2|}{|G_1|} \geqslant \frac{(p^4 - p^2)/2}{(p^3 - p)/\mu_1} = p\mu_1/2.$$

For $p > 2$ we have $p\mu_1/2 > 1$, while for $p = 2$ we have $V_1 \ni I$ by Remark 4.5; in both cases $V_1 \neq \langle O \rangle$. If, in addition, $\mu_1 > 2$ then $p\mu_1/2 > p$ and $\dim(V_1) > 1$. □

We conclude this subsection with yet another relation between the spaces V_s. Although it is not explicitly used in the present article, we include it for further references.

Proposition 4.9 *Let $M_1 \in V_{s_1}$ and $M_2 \in V_{s_2}$. Then $M_1 M_2 - M_2 M_1$ lies in $V_{s_1+s_2}$.*

Proof – By surjectivity of the reduction maps there exist matrices N_i with entries in $\mathbb{Z}/p^{s_j+1}\mathbb{Z}$ (where $\{i,j\} = \{1,2\}$) such that $X_i = I + p^{s_i} N_i \in G_{s_1+s_2+1}$ projects to $I + p^{s_i} M_i \in G_{s_i+1}$, which means that $N_i \equiv M_i \pmod p$. Then over the ring $\mathbb{Z}/p^{s_1+s_2+1}\mathbb{Z}$ we have

$$X_1X_2 - X_2X_1 = p^{s_1+s_2}(N_1N_2 - N_2N_1),$$

so that the commutator of X_1 and X_2 is

$$X_1X_2(X_2X_1)^{-1} = \left(X_2X_1 + p^{s_1+s_2}(N_1N_2 - N_2N_1)\right)(X_2X_1)^{-1} = I + p^{s_1+s_2}(N_1N_2 - N_2N_1),$$

which concludes the proof. □

The following property will be used in Section 5.

Proposition 4.10 *Let Γ be a congruence subgroup of exact level p^e and let Γ' be a congruence subgroup of exact level $p^{e'}$ with $\Gamma < \Gamma'$. Then the index $[\Gamma' : \Gamma]$ divides $p^{3e-2}(p+1)(p-1)$ and is divisible by $p^{e-e'}$.*

Proof – The first statement is obvious because $|\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})| = p^{3e-2}(p+1)(p-1)$. Further,

$$\Gamma = \Gamma_e \leqslant \Gamma_{e'} \leqslant \Gamma'_{e'} = \Gamma',$$

and by Corollary 4.6, for every $s < e$ we have $V_s \subsetneq \mathrm{sl}_2(\mathbb{F}_p)$, which implies that $[\Gamma_{s+1} : \Gamma_s]$ is divisible by p. Then $p^{e-e'}$ divides $[\Gamma_{e'} : \Gamma_e]$ and, a fortiori, $[\Gamma' : \Gamma]$. □

We are now ready to begin our inspection on groups of prime power level. We shall start with the groups such that $p \neq 2$ divides the order of G_1, then turn to those such that $p \neq 2$ does not divide the order of G_1, and finally consider the case $p = 2$.

4.4 The "unipotent" case

Throughout this and the following subsection we shall assume $p \neq 2$. In this subsection we consider groups Γ such that p divides the order of G_1. (One may call such Γ "unipotent".)

Assume that $\Gamma \ni -I$ and $\nu_\infty(\Gamma) \leqslant 2$. As follows from the results of Section 3, the group G_1 is either $\mathrm{SL}_2(\mathbb{F}_p)$ or $\mathrm{ST}_2(\mathbb{F}_p)$, up to conjugation.

We begin by studying the adjoint representations of $\mathrm{ST}_2(\mathbb{F}_p)$ and $\mathrm{SL}_2(\mathbb{F}_p)$, in order to find the subspaces of $\mathrm{sl}_2(\mathbb{F}_p)$ that are stable under their action.

Fix a generator g of the multiplicative group $\mathbb{F}_p^*$ and consider the matrices

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad X = \begin{pmatrix} g^{-1} & 0 \\ 0 & g \end{pmatrix}$$

in $\mathrm{SL}_2(\mathbb{F}_p)$. The element T generates the maximal unipotent group $\{\left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)\}$; the elements T and X, together, generate the special triangular group $\mathrm{ST}_2(\mathbb{F}_p)$; the three elements S, T, and X generate the special linear group[1] $\mathrm{SL}_2(\mathbb{F}_p)$.

We fix for $\mathrm{sl}_2(\mathbb{F}_p)$ the basis

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Proposition 4.11 *For $p \neq 2$ the only proper non-zero $\mathrm{ST}_2(\mathbb{F}_p)$-invariant subspaces of $\mathrm{sl}_2(\mathbb{F}_p)$ are $\langle B\rangle$ and $\langle A, B\rangle$. There are no proper non-zero $\mathrm{SL}_2(\mathbb{F}_p)$-invariant subspaces of $\mathrm{sl}_2(\mathbb{F}_p)$.*

Proof – We consider for $\mathrm{sl}_2(\mathbb{F}_p)$ the basis

$$e_1 = 4B, \quad e_2 = 2A, \quad e_3 = -A - 2C.$$

In this basis, the conjugation map $M \mapsto T^{-1}MT$ has the (left) matrix

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

[1] Actually, already S and T generate $\mathrm{SL}_2(\mathbb{F}_p)$, but it is more convenient for us to include X in the set of generators.

Hence the proper non-zero T-invariant subspaces of $\mathrm{sl}_2(\mathbb{F}_p)$ are $\langle e_1\rangle = \langle B\rangle$ and $\langle e_1, e_2\rangle = \langle A, B\rangle$. Since both are also X-invariant, they are $\mathrm{ST}_2(\mathbb{F}_p)$-invariant, and there are no other. Since none of them is S-invariant, there is no non-zero proper invariant $\mathrm{SL}_2(\mathbb{F}_p)$-subspaces. □

This proposition allows us to settle the case $G_1 = \mathrm{SL}_2(\mathbb{F}_p)$, for $p > 2$.

Corollary 4.12 *Let Γ be of level p^e with $p \neq 2$. Assume that $\Gamma \ni -I$, that $\nu_\infty(\Gamma) \leqslant 2$ and that $G_1 = \mathrm{SL}_2(\mathbb{F}_p)$. Then $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.*

Proof – Propositions 4.3, 4.8 and 4.11 imply $V_1 = \mathrm{sl}_2(\mathbb{F}_p)$, and we conclude by Corollary 4.6. □

Now we are ready to classify all "unipotent" Γ of odd prime power level, such that

$\Gamma \ni -I$, and every congruence subgroup of Γ containing the elliptic elements of Γ has at most 2 cusps (7)

Proposition 4.13 *Let Γ be a congruence subgroup of exact level p^e, with $e > 1$ and $p \neq 2$, such that p divides $|G_1|$. Assume that Γ satisfies (7). Then we have one of the following two cases:*

- *Γ is of exact level 9 and the curve X_Γ is of genus 0;*
- *Γ is of exact level 27 and the curve X_Γ is of genus 1.*

(In both cases Γ is uniquely defined up to conjugacy.)

Together with Theorem 2.2 this has the following consequence.

Corollary 4.14 *Let Γ be a congruence subgroup of exact level p^e, with $e > 1$ and $p \neq 2$, such that p divides $|G_1|$. Then either Siegel's theorem is effective for X_Γ or X_Γ is non-Siegelian.*

Remark 4.15 One can give a totally explicit description for the groups Γ from Proposition 4.13. For instance, for the Γ of level 9, the group G_2 is, up to conjugacy generated by the matrices

$$\begin{pmatrix} 2 & -1 \\ 3 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & -2 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z}).$$

One can exhibit a similar set of generators for the group G_3 which defines the Γ of level 27; see [10, Proposition 7.3.5] for the missing details.

Proof of Proposition 4.13 – If Γ contains $-I$ and has at most 2 cusps, then so does Γ_1, and by Theorem 3.6 we may assume that either $G_1 = \mathrm{SL}_2(\mathbb{F}_p)$ or $G_1 = \mathrm{ST}_2(\mathbb{F}_p)$. The former case is impossible by Corollary 4.12, so we have $G_1 = \mathrm{ST}_2(\mathbb{F}_p)$.

Next, let G' be the subgroup of $\mathrm{ST}_2(\mathbb{F}_p)$ generated by elements of order dividing 12, and let Γ' be the intersection of Γ with the pull-back of G' to $\mathrm{SL}_2(\mathbb{Z})$. Then Γ' contains $-I$ and the elliptic elements of Γ. On the other hand, for $p \notin \{2, 3, 5, 7, 13\}$ the group G' is a proper subgroup of $\mathrm{ST}_2(\mathbb{F}_p)$, and Proposition 3.5 implies that Γ'_1 has at least 3 cusps. Hence so does Γ'. We conclude that $p \in \{3, 5, 7, 13\}$.

The group Γ contains $-I$, has at most two cusps, and satisfies $\mu(\Gamma_1) = p + 1$. Proposition 4.8 implies $\dim(V_1) \geqslant 2$. By Proposition 4.3, Proposition 4.11 and Corollary 4.6 we obtain $V_1 = \langle A, B\rangle$, and Proposition 4.4 gives $V_1 = V_2 = \ldots = V_{e-1}$. Hence $|G_e| = p^{2e}(1 - p^{-1})$.

On the other hand, Corollary 2.4 and (1) imply that any subgroup Γ' of Γ that contains $-I$ and has at most 2 cusps must satisfy $|G'_e| \geqslant |\mathcal{M}_{p^e}|/2 = p^{2e}(1 - p^{-2})/2$. Thus,

$$[G_e : G'_e] \leqslant \frac{p^{2e}(1 - p^{-1})}{p^{2e}(1 - p^{-2})/2} = \frac{2}{1 + p^{-1}} < 2.$$

This implies that if Γ satisfies (7) then any proper subgroup of Γ of the exact level p^e, containing $-I$, cannot have at most two cusps. In particular, if Γ satisfies (7) then the congruence subgroup generated by $\Gamma(p^e)$, by $-I$, and by the elliptic elements of Γ is Γ itself.

A direct verification on the levels 3^4, 5^2, 7^2, and 13^2 shows that there exist no groups Γ with this property, with at most two cusps, and such that $G_1 = \mathrm{ST}_2(\mathbb{F}_p)$. A further inspection on the levels 3^2 and 3^3 concludes our classification. See [10, Section 4.3] for more details.

If Γ does not satisfy (7) then Siegel's theorem is effective for X_Γ by Theorem 2.2. If Γ satisfies (7) then either X_Γ has genus 1, and Siegel's theorem is effective for X_Γ by Theorem 1.2, or X_Γ has genus 0, and is non-Siegelian. □

4.5 The "semi-simple" case

As in the previous subsection, we assume $p \neq 2$. In this subsection we consider groups Γ such that p does not divide the order of G_1. (One may call such Γ "semi-simple".) As we have seen in Section 3, up to conjugacy there are ten possible groups G_1 for $p \neq 2$.

We shall need a simple lemma, that will be used for $n = 3$, but we state the general case. It is certainly well-known, but we include a proof for the sake of completeness.

Lemma 4.16 *Let A be an algebra over a field of characteristic distinct from 2, and let $X_1, \dots, X_n$ be invertible and pairwise anti-commuting*[2] *elements of A. Then $X_1, \dots, X_n$ are linearly independent over the base field.*

Proof – Let $S = \sum_i a_i X_i$ be a linear combination of the X_i, with a_i in the base field. If $S = 0$ then for every i we have

$$0 = X_i S + S X_i = \sum_{j \neq i} a_i (X_i X_j + X_j X_i) + 2a_i X_i^2 = 2a_i X_i^2.$$

Since X_i is invertible in A and 2 is invertible in the base field, this implies that every a_i is 0. □

Now we have the following property, which allows us to exclude immediately seven of the ten cases referred to in the beginning of this subsection.

Proposition 4.17 *Let G be a subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$ and let $\bar{G}$ be its image in $\mathrm{PSL}_2(\mathbb{F}_p)$. If $\bar{G}$ contains a subgroup $\bar{H}$ isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then $\mathrm{sl}_2(\mathbb{F}_p)$ has a basis consisting of three elements of G.*

If $\bar{G}$ contains a subgroup isomorphic to the alternating group $\mathcal{A}_4$, then there are no non-trivial G-stable subspaces of $\mathrm{sl}_2(\mathbb{F}_p)$.

Proof – Let $\bar{X}$ and $\bar{Y}$ be generators of $\bar{H} \equiv \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and let $\pm X$ and $\pm Y$ be their pullbacks in G. Since the elements X, Y, and XY are traceless, they belong to $\mathrm{sl}_2(\mathbb{F}_p)$. The obvious relations $X^2 = Y^2 = (XY)^2 = -I$ show that X, Y, and XY are pairwise anti-commuting as in Lemma 4.16. Hence they form a basis of $\mathrm{sl}_2(\mathbb{F}_p)$.

In this basis, the conjugation maps by X, Y, and XY have the matrices

$$\gamma_X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \qquad \gamma_Y = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \qquad \gamma_{XY} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

This implies that the G-invariant subspaces of $\mathrm{sl}_2(\mathbb{F}_p)$ are generated by subsets of $\{X, Y, XY\}$.

Let now $\bar{G}$ contain a subgroup isomorphic to $\mathcal{A}_4$; in turn, this will contain a subgroup $\bar{H}$ isomorphic to the Klein group $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and an element $\bar{R}$ that cycles, by conjugation, the non-trivial elements of $\bar{H}$. Taking a basis X, Y, and XY of $\mathrm{sl}_2(\mathbb{F}_p)$ as above, the pullback R of $\bar{R}$ in G cycles the spaces $\langle X \rangle$, $\langle Y \rangle$, and $\langle XY \rangle$. Thus the only G-invariant subspaces of $\mathrm{sl}_2(\mathbb{F}_p)$ are trivial. □

Proposition 4.18 *Let Γ be a congruence subgroup of exact level p^e, with $e > 1$ and $p \neq 2$, such that p does not divide $|G_1|$. Assume that Γ contains $-I$ and has at most two cusps. Then we have one of the following cases:*

- *$p^e = 9$, $\bar{G}_1 = \mathcal{C}_2$ and the curve X_Γ is of genus 0;*
- *$p^e = 9$, $\bar{G}_1 = \mathcal{D}_2$ and the curve X_Γ is of genus 0;*
- *$p^e = 25$, $\bar{G}_1 = \mathcal{D}_3$ and the curve X_Γ is of genus 2.*

(In all three cases the group Γ is uniquely defined up to conjugacy.)

Together with Theorem 2.1 this has the following consequence.

Corollary 4.19 *Let Γ be a congruence subgroup of exact level p^e, with $e > 1$ and $p \neq 2$, and such that p does not divide $|G_1|$. Then either Siegel's theorem is effective for X_Γ, or X_Γ is non-Siegelian, or $p^e = 25$.* □

[2]that is, $X_i X_j + X_j X_i = 0$ for $i \neq j$

Remark 4.20 Again, one can give a more explicit description for the three groups Γ above. For instance, for the "wicked" Γ of level 25, the group G_2 is, up to conjugacy, generated by the matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 7 \\ 7 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 5 \\ -5 & 1 \end{pmatrix}, \begin{pmatrix} 11 & -5 \\ 0 & -9 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/25\mathbb{Z}).$$

One has a similar description for the two groups of level 9; see [10, Proposition 7.4.4].

Proof of Proposition 4.18 – If Γ contains $-I$ and has at most 2 cusps, then then so does Γ_1. Theorem 3.6 now implies that, up to conjugacy, G_1 is one of the ten groups with $p \neq 2$ in Table 1(a). We also have $\mu(G_1) > 2$, which implies $\dim(V_1) \geqslant 2$ by Proposition 4.8. Now the seven groups corresponding to the final four lines of Table 1(a) can be excluded using Proposition 4.3, Proposition 4.17 and Corollary 4.6.

We are left with the cases when either $p = 3$ and $\bar{G}_1 \cong \mathcal{C}_2$, or $p = 3$ and $\bar{G}_1 \cong \mathcal{D}_2$, or $p = 5$ and $\bar{G}_1 \cong \mathcal{D}_3$. A direct verification on the levels 3^3 and 5^3 shows that there exist no groups Γ of these exact levels that contain $-I$, have at most 2 cusps and such and such that p does not divide $|G_1|$. A further inspection on the levels 3^2 and 5^2 concludes our classification.

We conclude the proof using Theorem 2.1. □

4.6 The case $p = 2$

In this subsection we assume $p = 2$, that is, G_1 is a subgroup of $\mathrm{SL}_2(\mathbb{F}_2) \cong \mathcal{S}_3$. The following propositions are proved by inspection on the levels 2^s for $s \leqslant 6$. For the details see [10, Section 7.5].

Proposition 4.21 *Let Γ be a congruence subgroup of exact order 2^e with $e > 1$ and with $G_1 \cong \mathcal{C}_2$. Assume that Γ contains $-I$ and satisfies* (7). *Then $e \leqslant 5$ and Γ is uniquely determined by e up to conjugacy. For $2 \leqslant e \leqslant 4$ the curve X_Γ is non-Siegelian, while for $e = 5$ the curve X_Γ is Siegelian and has genus* 1. □

Proposition 4.22 *Let Γ be a congruence subgroup of exact level 2^e with $e > 1$ and with $G_1 \cong \mathcal{C}_3$. Assume that Γ contains $-I$ and satisfies* (7). *Then $e \leqslant 4$ and Γ is uniquely determined by e up to conjugacy. Moreover X_Γ is non-Siegelian.* □

Proposition 4.23 *Let Γ be a congruence subgroup of exact level 2^e, for some $e > 1$, containing $-I$, having at most 2 cusps and with $G_1 = \mathrm{SL}_2(\mathbb{F}_2)$. Then $e \leqslant 4$ and Γ belongs to one of eight distinct conjugacy classes. For each of them X_Γ is non-Siegelian.* □

Together with Theorems 1.2 and 2.2, the above results have the following consequence.

Corollary 4.24 *Let Γ be a congruence subgroup of exact level 2^e with $e > 1$. Then either Siegel's theorem is effective for X_Γ or X_Γ is non-Siegelian.* □

Theorem 1.3 is a combination of Theorem 3.1 and Corollaries 4.14, 4.19 and 4.24.

The complete least of non-Siegelian curves of exact level p^e with $e > 1$ is given in Table 2.

5 The Mixed Levels

In this section we study groups of mixed level. Our goal is to prove Theorem 1.4. Let Γ be a congruence subgroup of exact level n, and let the factorization of n be

$$n = \prod_{i \in I} q_i = \prod_{i \in I} p_i^{e_i},$$

where the p_i are distinct primes and $e_i > 0$ for every $i \in I$. For every positive integer d we denote by Γ_d the composite group $\Gamma \cdot \Gamma(d)$, of level dividing d, and by $G_d < \mathrm{SL}_2(\mathbb{Z}/d\mathbb{Z})$ its projection modulo d. The group $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to the direct product $\prod_{i \in I} \mathrm{SL}_2(\mathbb{Z}/q_i\mathbb{Z})$; this allows us to consider $G = G_n$ as a subgroup of the direct product $\prod_{i \in I} G_{q_i}$.

Remark 5.1 1. If $n = p^e$ then G_s and Γ_s of Section 4 become G_{p^s} and Γ_{p^s} in this section.

Table 2: Non-Siegelian modular curves X_Γ of exact prime power level p^e with $e > 1$

p^e	Γ_1	μ	ν_∞	ν_2	ν_3	$\mathbf{g}$	remark
4	$G_1 \cong \mathcal{C}_2$	6	2	2	0	0	
8		12	2	4	0	0	
16		24	2	8	0	0	
4	$G_1 \cong \mathcal{C}_3$	8	2	0	2	0	
8		16	2	0	4	0	
16		32	2	0	8	0	
4	$\Gamma_1 = \Gamma(1)$	4	1	2	1	0	
8		16	2	4	1	0	
8		8	1	2	2	0	2 groups
16		16	1	2	4	0	4 groups
9	$\Gamma_1 = \Gamma_0(3)$	12	2	0	3	0	
9	$\bar{G}_1 \cong \mathcal{C}_2$	18	2	6	0	0	
9	$\bar{G}_1 \cong \mathcal{D}_2$	9	1	5	0	0	

2. If Siegel's theorem is effective for Γ_d then it is effective also for Γ.
3. Notice that for $d \neq n$ the group Γ_d is not obliged to have the exact level d, even if d divides n; as in Remark 4.2, *a priori* we only know that Γ_d is of level dividing d.

5.1 Proof of Theorem 1.4

We begin with the following useful observation. Let $\{S_i\}_{i\in I}$ be a finite family of finite groups S_i and let $S = \prod_{i\in I} S_i$ be their direct product. For a subset $J \subset I$ we view $S_J = \prod_{i\in J} S_i$ as a subgroup of S, and we denote by $\pi_J \colon S \to S_J$ the natural projection.

Proposition 5.2 *Let T be a subgroup of S, and let T_J and U_J be the subgroups of S_J defined by $T_J = \pi_J(T)$ and $U_J = T \cap S_J$. Then U_J is a normal subgroup of T_J. Let also r_i be the index of $U_{\{i\}}$ in $T_{\{i\}}$. Then r_j divides $\prod_{i\neq j} r_i$ for every $j \in I$.*

Proof – Let $I = J \cup K$ be a partition of I. The group $U_J = \mathrm{Ker}(\pi_K|_T)$ is normal in T; then $U_J = \pi_J(U_J)$ is a normal subgroup of $T_J = \pi_J(T)$. The composite map $T \twoheadrightarrow T_J \twoheadrightarrow T_J/U_J$ has kernel $U_J \times U_K$ and induces an isomorphism $T/(U_J \times U_K) \cong T_J/U_J$, which proves $T_J/U_J \cong T_K/U_K$.

Now note that

$$\prod_{i\in K} U_{\{i\}} < U_K < T_K < \prod_{i\in K} T_{\{i\}}.$$

This implies that $|T_K/U_K|$ divides $\left|\prod_{i\in K} T_{\{i\}} / \prod_{i\in K} U_{\{i\}}\right| = \prod_{i\in K} r_i$. Taking $J = \{j\}$, we obtain $T_{\{j\}}/U_{\{j\}} \cong T_K/U_K$, whence the result. □

Applying the above proposition to the group $G < \prod_{i\in I} G_{q_i}$ we obtain the following.

Corollary 5.3 *Let Γ be a congruence subgroup of exact level $n = \prod_{i\in I} q_i$. Then for every $i \in I$ the congruence subgroup $(\Gamma \cap \Gamma(n/q_i)) \cdot \Gamma(q_i)$ of exact level q_i projects modulo q_i onto a normal subgroup H_{q_i} of G_{q_i} of index r_i, and r_j divides $\prod_{i\neq j} r_i$ for every $j \in I$.* □

The next statement is certainly well-known, but we include a proof for the sake of completeness.

Proposition 5.4 *Let p be a prime and let H_s be a normal subgroup of $\mathrm{SL}_2(\mathbb{Z}/p^s\mathbb{Z})$ for some $s > 0$. If $H_s \neq \mathrm{SL}_2(\mathbb{Z}/p^s\mathbb{Z})$ then p divides the index of H_s.*

Proof – When $s = 1$, the cases $p \leqslant 3$ are verified by inspection, and for $p \geqslant 5$ any proper normal subgroup of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is contained in $\{\pm I\}$. For $s > 1$, the projection of H_s modulo p^{s-1} is a normal subgroup H_{s-1} of $\mathrm{SL}_2(\mathbb{Z}/p^{s-1}\mathbb{Z})$, and $[\mathrm{SL}_2(\mathbb{Z}/p^s\mathbb{Z}) : H_s] = p^a[\mathrm{SL}_2(\mathbb{Z}/p^{s-1}\mathbb{Z}) : H_{s-1}]$ for some $a \geqslant 0$. We conclude by induction. □

This has the following consequence.

Proposition 5.5 *Let Γ be congruence subgroup of exact level n, let $p > 3$ be the largest prime divisor of n and let q be the exact power of p dividing n. Then $G_q \neq \mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$.*

Proof – Let G_q and H_q be as in Corollary 5.3. Since p does not divide $\left|\mathrm{SL}_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z})\right|$ for any prime $p_i < p$, it cannot divide $[G_q : H_q]$ by Corollary 5.3. Proposition 5.4 now implies that if $G_q = \mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$ then $H_q = G_q$, but in this case p would not divide n. □

Corollary 5.6 *Let Γ and p be as in Proposition 5.5. Assume that $p > 13$. Then Siegel's theorem is effective for X_Γ.*

Proof – As above, let q be the exact power of p dividing n, and consider the congruence subgroup $\Gamma_q = \Gamma \cdot \Gamma(q)$ of level dividing q. Since $p > 13$, the results of the previous sections imply that either Siegel's theorem is effective for X_{Γ_q} or $G_q = \mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$, which contradicts Proposition 5.5. □

Proof of Theorem 1.4 – Let Γ be a subgroup of exact level $n = \prod p^{e_p}$. If the set of prime divisors of n is not contained in $\{2, 3, 5, 7, 11, 13\}$ then we conclude by Corollary 5.6. Assume now that n factors in the primes $2, 3, 5, 7, 11, 13$.

For every prime p let $\Gamma_{(p)} = (\Gamma \cap \Gamma(n/p^{e_p})) \cdot \Gamma(p^{e_p})$ and $\Gamma'_{(p)} = \Gamma_{p^{e_p}} = \Gamma \cdot \Gamma(p^{e_p})$ be the congruence subgroups of Corollary 5.3, of exact levels respectively p^{e_p} and $p^{e'_p}$, and with $\Gamma_{(p)} < \Gamma'_{(p)}$. Put also $r_p = [\Gamma'_{(p)} : \Gamma_{(p)}]$.

If Siegel's theorem is effective for $X_{\Gamma'_{(p)}}$ then it is effective for X_Γ, too. Otherwise, by the results of the previous sections, we have $e'_2 \leqslant 4$, $e'_3, e'_5 \leqslant 2$, and $e'_7, e'_{11}, e'_{13} \leqslant 1$.

We are now going to find a bound for e_2. By Corollary 5.3 we have that r_2 divides $\prod_{p\neq 2} r_p$. By Proposition 4.10 we obtain that $2^{e_2 - e'_2}$ divides r_2 and that $\prod_{p\neq 2} r_p$ divides $\prod_{p\neq 2} p^{3e_p-2}(p+1)(p-1)$. Thus $2^{e_2-e'_2}$ divides $\prod_{p\leqslant 13}(p+1)(p-1)$ which implies $e_2 - e'_2 \leqslant 16$. Since $e'_2 \leqslant 4$, we obtain $e_2 \leqslant 20$.

In exactly the same way we bound the other exponents e_p, completing thereby the proof. □

References

[1] P. Alvanos and Yu. Bilu and D. Poulakis, Characterizing algebraic curves with infinitely many integral points, *Int. J. Number Theory* **5** (2009), 1–6.

[2] A. Baker and J. Coates, Integer points on curves of genus 1, *Proc. Cambridge Philos. Soc.* **67** (1970), 595–602.

[3] Yu. F. Belotserkovskiĭ (Yu. Bilu), Effective analysis of a new class of Diophantine equations. (Russian. English summary) *Vestsi Akad. Navuk BSSR Ser. Fiz.-Mat. Navuk* **125**, (1988), 34–39.

[4] Yu. Bilu, Effective analysis of integral points on algebraic curves, *Israel J. Math.* **90** (1995), 235–252.

[5] Yu. Bilu, Baker's method and modular curves, *A Panorama of Number Theory or The View from Baker's Garden* (edited by G. Wustholz), 73–88, Cambridge University Press, 2002.

[6] P. Corvaja, U. Zannier, A Subspace Theorem approach to integral points on curves, *C. R. Acad. Sci. Paris Ser. I* **334** (2002), 267–271.

[7] R. Dvornicich and U. Zannier, Fields containing values of algebraic function, *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **21** (1994), 421–443.

[8] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366.

[9] D. S. Kubert and S. Lang, *Modular Units*, Grundlehren math. Wiss. **244**, Springer, New York, 1981.

[10] M. Illengo, *Diophantine Analysis and Linear Groups*, Ph. D. Thesis, Pisa - Bordeaux 2008, `http://grenet.drimm.u-bordeaux1.fr/pdf/2008/ILLENGO_MARCO_2008.pdf`

[11] S. Lang, *Introduction to modular forms*, Grund. math. Wiss. **222**, Springer, Berlin-New York, 1976.

[12] S. Lang *Fundamentals of Diophantine geometry*, Springer-Verlag, New York, 1983

[13] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.

[14] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, 3rd edition, Vieweg & Sohn, Braunschweig/Wiesbaden, 1997

[15] C. L. Siegel, Über einige Anwendungen Diophantischer Approximationen, *Abh. Preuss Akad. Wiss. Phys.-Math. Kl.*, 1929, Nr. 1; *Ges. Abh.*, Band 1, 209–266.

[16] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan **11**, Kanô memorial lectures, **1**, Iwami Shoten Publishers and Princeton University Press, 1971.